UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA

UMG RECORDINGS, INC., *et al.*, *Plaintiffs*, v. KURBANOV, *et al.*, *Defendants*.	Case No. 1:18-cv-00957-CMH-TCB

REPLY IN SUPPORT OF PLAINTIFFS' MOTION TO COMPEL PRESERVATION AND PRODUCTION OF WEB SERVER DATA

Defendant does not dispute that the web server data at issue exists and is relevant. Indeed, the server data is essential to the operation of Defendant's Websites and identifies the YouTube videos that are stream-ripped, the MP3 files that are copied and distributed, and the geographic locations of the users downloading the audio files. Instead, Defendant opposes Plaintiffs' motion by obscuring the issues before the Court. He refuses to accept the basic definition of electronically stored information ("ESI") under Federal Rule of Civil Procedure 34. He also raises privacy and other concerns that are easily resolved.

The issue before the Court is whether Defendant will flip a switch on his *web server* software so that the data at issue will be saved rather than erased. The requested preservation of server data can occur locally, on Defendant's web server software using its already built-in functionality. As set forth in the declaration of Robert W. Schumann attached to Plaintiffs' motion, logging using web server software is routine among website operators, and something Defendant can do easily. (Pls.' Mem. at 7; Schumann Decl. ¶¶ 12–14). Notably, Defendant does not deny that, to preserve the server data at issue, he can simply enable logging on his web server software.

Defendant confuses matters by discussing his custom-made *website* software—which is distinct from the standard web server software that underlies it—and what is allegedly involved with re-programming that website software. (Kurbanov Decl. ¶¶ 7–9; Opp'n at 1, 4). Defendant further confuses matters by making assertions about his alleged practices concerning storage of stream-ripped *audio files*. (Kurbanov Decl. ¶¶ 10–11; Opp'n at 5). But Plaintiffs seek Defendant's preservation and production of *web server data logs*, using his *web server* software. Defendant's allegations about his website software and the audio files themselves thus are irrelevant.

Relatedly, Defendant repeatedly argues that he should not be required to "create" data that does not already "exist." But preserving ESI is not tantamount to creating documents that do not otherwise exist. (Pls.' Mem. at 9–11). The server data exists (until it is erased); Defendant's Websites otherwise could not function. (Schumann Decl. ¶¶ 9–11). Despite his obfuscation, Defendant gives away the game deep into his opposition where he finally concedes "the data with which such files could be created *does exist*." (Opp'n at 13 (emphasis added)). Respectfully, Plaintiffs' motion should be granted.

I. The Server Data Is ESI

There is no merit to Defendant's arguments that the server data at issue is too ephemeral to constitute ESI under Federal Rule of Civil Procedure Rule 34(a). Rule 34(a)(1) "is expansive," "includes any type of information that is stored electronically," and covers information "stored in any medium." Fed. R. Civ. P. 34(a) advisory committee's note to 2006 amendment, ¶ 2. "Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined." *Id.* ¶ 2. Courts have deemed RAM copies sufficiently fixed. *See*, *e.g.*, *Columbia Pictures, Inc. v.*

Bunnell, 245 F.R.D. 443, 446–48 (C.D. Cal. 2007) (ordering defendant to preserve and produce server log data that was temporarily stored in RAM); *Quantum Sys. Integrators, Inc. v. Sprint Nextel Corp.*, 338 F. App'x 329, 337 (4th Cir. 2009) (unpublished) (finding that RAM copies are "sufficiently fixed for purposes of copyright infringement").

Defendant's main case, *Paramount Pictures Corp. v. Replay TV*, 2002 U.S. Dist. LEXIS 28126 (C.D. Cal. May 30, 2002), is inapposite. *Replay TV* involved a demand regarding data on devices at users' locations, not data that a defendant received, processed, and responded to on its own servers. Indeed, *Bunnell* rejected the same argument that Defendant now makes regarding *Replay TV*, holding that "because the Server Log Data already exists, is temporarily stored in RAM, and is controlled by defendants, an order requiring defendants to preserve and produce such data is not tantamount to ordering the creation of new data." *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *6 (C.D. Cal. May 29, 2007).[1]

Defendant's other cases are also of no moment. None involves a motion to preserve evidence or otherwise precludes production of "ephemeral" data, much less data similar to the server data at issue here. *See Louis Vuitton Malletier v. Dooney & Bourke, Inc.*, No. 04 Civ. 5316 RMB MHD, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (sanctions motion regarding communications in customer relations chat room); *Convolve, Inc. v. Compaq Comput. Corp.*, 223 F.R.D. 162, 176–77 (S.D.N.Y. 2004) (request for sanctions for not preserving data reflecting adjustments by a tuning engineer to a device); *Williams v. UnitedHealth Grp.*, No. 2:18-cv-2096, 2020 WL 528604, at *2 (D. Kan. Feb. 3, 2020) (discovery motion regarding instant messages, without addressing the scope of preservation obligations); *King v. Catholic*

[1] Notably, the court in *Replay TV* issued its decision in 2002, well before the 2006 amendments to the Federal Rules of Civil Procedure explicitly incorporated provisions concerning ESI. Unlike the court in *Bunnell*, the *Replay TV* court did not have the benefit of these new provisions or the advisory committee's accompanying guidance.

Health Initiatives, No. 8:18CV326, 2019 WL 6699705, at *4–5 (D. Neb. Dec. 9, 2019) (requiring defendants to supplement their production with emails, not instant messages, in response to request for sanctions).

II. Defendant's Privacy and Burden Arguments Fail

A. Privacy

Defendant has not established that producing the requested data requires him to violate privacy laws or put users of his Websites at risk. In fact, he has not raised any credible arguments toward that end.

First, the Privacy Policy for Defendant's Websites informs users that the server data at issue may be collected and disclosed.[2] When the users affirmatively opt into the click-through agreement before each "convert" request, they assent to Defendant's Terms of Use and its incorporated Privacy Policy.[3] Thus, users have given their consent to collection and disclosure of the data, and should not expect that their activity on Defendant's Websites is not logged or disclosed.

[2] "Using the Service. When you access the Service, use the search function, convert files or download files, your IP address, country of origin and other non-personal information about your computer or device (such as web requests, browser type, browser language, referring URL, operating system and date and time of requests) may be recorded for log file information, aggregated traffic information and in the event that there is any misappropriation of information and/or content. Usage Information. We may record information about your usage of the Service such as your search terms, the content you access and download and other statistics. . . . Disclosure of Information[.] We may be required to release certain data to comply with legal obligations or in order to enforce our Terms of Use and other agreements. We may also release certain data to protect the rights, property or safety of us, our users and others. This includes providing information to other companies or organizations like the police or governmental authorities for the purposes of protection against or prosecution of any illegal activity, whether or not it is identified in the Terms of Use." FLVTO.biz, "Privacy Policy," https://www.flvto.biz/en95/policy/ (last visited June 23, 2021); *see also*2conv.com, "Privacy Policy," https://2conv.com/en80/policy/ (last visited June 23, 2021) (same).

[3] To convert a file, a user must check a box agreeing that "[b]y using our service you are accepting our Terms of Use." FLVTO.biz, "FLVTO," https://www.flvto.biz/en96/ (last visited June 24, 2021); *see also* 2conv.com, "2conv," https://2conv.com/en81/ (last visited June 24, 2021) (same). The Terms of Use provide in relevant part: "We retain a separate Privacy Policy and your assent to these Terms also signifies your assent to the Privacy Policy." FLVTO.biz, "Terms of Use," https://www.flvto.biz/en96/terms/ (last visited June 24, 2021); 2conv.com, "Terms of Use," https://2conv.com/en81/terms/ (last visited June 24, 2021) (same).

Second, Defendant argues that preservation and disclosure of IP addresses "would likely violate the laws of Germany." (Opp'n at 18). But Defendant's own brief indicates that individuals in Germany can consent to the collection and use of the data, and Defendant has structured Defendant's Websites to obtain that consent. (Opp'n at 18; *see supra* nn.2–3). In any event, a party relying on foreign law has the burden of showing that such law bars the discovery at issue. *United States v. Vetco,* 691 F.2d 1281, 1289 (9th Cir. 1981). Defendant has not made that showing.

Third, Defendant hypothesizes that, if he is required to preserve server data logs, those logs could expose "dissident material" to the Russian government. (Opp'n at 6). But he offers no basis to believe that his stream-ripping sites are used for purposes of political dissent. Defendant's speculation is not a substitute for facts. Moreover, his hypothetical scenario is highly unlikely given that the Russian government has ordered internet service providers in that country to block access to the www.flvto.biz site. And, as explained above, Plaintiffs are seeking preservation of server data logs, not the audio files themselves.

Fourth, and finally, any privacy concerns can be further mooted by Defendant redacting the specific IP addresses (or replacing them with unique but anonymous identifiers), while still providing server data identifying: the YouTube videos that are stream-ripped, the MP3 files that are copied and distributed, and whether the users that downloaded the audio files are in the United States or elsewhere. Defendant's only purported privacy concern relates to IP addresses; redactions, combined with identification of the user's geographical location, can readily address that concern.

B. Burden

Defendant's does not expressly argue that producing the requested data presents an undue burden. Nonetheless, in an abundance of caution, Plaintiffs address a pair of his assertions in this area.

First, Defendant asserts that storage costs for preserving the server data could cost $4,500 per year using Amazon Web Services ("AWS"). It is unclear why Defendant cites AWS costs, rather than the lower costs of storing the requested data on a local hard drive. It is also unclear why Defendant quotes the storage costs on a yearly basis. Discovery is set to close on August 13, 2021, and Plaintiffs need an adequate sample only. But, even if the storage expense is $4,500, that amount is plainly "proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, [and] the parties' resources." Fed. R. Civ. Pro. 26(b). The likely benefit of the information easily outweighs the expense of a few thousand dollars. *Id.* The manner in which Defendant has litigated this case to date suggests that he can afford this expense. Nonetheless, if the Court deems it necessary, Plaintiffs are willing to pay the $4,500 (or a lesser amount) as an alternative.

Second, Defendant asserts that it is his "understanding and belief" that changing the setting on his web server software "would cause the Websites to run more slowly." (Kurbanov Decl. ¶ 6). However, Defendant's statement is unreliable. Defendant offers no basis for his conclusory assertion. Courts routinely decline to accept unsubstantiated, merely conclusory statements in declarations. *See, e.g.*, *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 2020 WL 2312030, at *10 (E.D. Va. May 8, 2020) (refusing to rely on "conclusory" statement in declaration regarding financial impact of injunction); *It's My Party, Inc. v. Live Nation, Inc.*, 2012 WL

3655470, at *4 (D. Md. Aug. 23, 2012) (striking declaration testimony that "appear[ed] to be based on speculation rather than personal knowledge"). Defendant repeatedly refused to discuss with Plaintiffs the web server software that he uses. In his 5-page declaration, Defendant continues to play games, once again withholding the name of his web server software. (Kurbanov Decl. ¶ 6). Significantly, even though Defendant raises one baseless argument after another, he does not dispute that he uses Nginx web server software—this is a popular program with *built-in functionality for saving server data in a log*. (Pls.' Mem. at 8; Schumann Decl. ¶ 18). Defendant also concedes that it is commonplace for websites to log server activity. (Pls.' Mem. at 7; Schumann Decl. ¶ 12). It is difficult to fathom that preserving server data (in the form of logs) would be so common if it negatively impacted site performance.

C. Yandex Metrica

Defendant's privacy and burden arguments fall flat for another compelling reason. Defendant has not disputed that, apart from any local logging using his web server software, he already is engaged in remote logging with a third-party service. Defendant's arguments in opposition to Plaintiffs' motion, including as to privacy and burden, thus are pretextual.

Defendant has integrated Yandex Metrica into the program code of his Websites, capturing and storing data concerning various events, including each "convert" request and each "MP3 download" request. (Pls.' Mem. at 8; Schumann Decl. ¶¶ 16–18). Yandex Metrica has sophisticated reporting capabilities, accessible to Defendant via an online dashboard. (Pls.' Mem. at 7; Schumann Decl. ¶ 14). Defendant is obligated to access that data in his possession and control at Yandex Metrica and produce it.

Except for Defendant's unwillingness to participate in discovery, none of this should be controversial or difficult. Indeed, Defendant accessed and used his logged data at Yandex

Metrica to support a prior declaration that he again relied upon in his opposition. (*See* ECF No. 25-1, Ex. 2;[4] Opp'n at 3–4; Kurbanov Decl. ¶ 5). One way or the other, Defendant should be ordered to produce the requested server data identifying: the YouTube videos that are stream-ripped, the MP3 files that are copied and distributed, and whether the users downloading those audio files are in the United States or elsewhere.

CONCLUSION

For the reasons discussed above, Plaintiffs respectfully request that the Court grant the relief requested herein.

Respectfully submitted,

Dated June 24, 2021

/s/ Scott A. Zebrak
Scott A. Zebrak (VSB No. 38729)
Matthew J. Oppenheim (*pro hac vice*)
Lucy Grace D. Noyola (*pro hac vice*)
Kellyn M. Goler (*pro hac vice*)
OPPENHEIM + ZEBRAK, LLP
4530 Wisconsin Avenue, NW, 5th Floor
Washington, DC 20016
Tel: (202) 480-2999
Fax: (866) 766-1678
scott@oandzlaw.com
matt@oandzlaw.com
lucy@oandzlaw.com
kellyn@oandzlaw.com

Attorneys for Plaintiffs

[4] Attached as Exhibit A is a copy of the Declaration of Tofig Kurbanov in Support of Motion to Dismiss (ECF No. 25-1).